UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/640,453	08/17/2000	William C. Arnold	YOR9-2000-0331	4496

29683　　　7590　　　03/24/2005	**EXAMINER**	
HARRINGTON & SMITH, LLP	FIELDS, COURTNEY D	
4 RESEARCH DRIVE		
SHELTON, CT 06484-6212	**ART UNIT**	**PAPER NUMBER**
	2137	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

HL

	Application No.	**Applicant(s)**
	09/640,453	ARNOLD ET AL.
Office Action Summary	**Examiner**	**Art Unit**	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>08 November 2004</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-46</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-46</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

Response to Arguments

1.   Applicant's arguments, see pages 3-6, filed 08 November 2004, with respect to

the rejection(s)of claim(s) 1-46 under Chi (U.S. Patent No. 5,979,917), McLain, Jr. (U.S.

Patent No. 5,812,826), and Chambers (U.S. Patent No. 5,398,196) have been fully

considered and are persuasive. Therefore, the rejection has been withdrawn.

However, upon further consideration, a new ground(s) of rejection is made in view of

Schnurer et al (U.S. Patent No. 5,842,002) and Nachenberg (U.S. Patent No.

5,826,013).

DETAILED ACTION

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

3.   Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention. It is unclear how the network can be isolated if it's connected

to another network. Please clarify.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Schnurer et al (U.S. Patent No. 5,842,002) and further in view of Nachenberg (U.S.

Patent No. 5,826,013).

As per claim 1, Schnurer et al. teaches a system for monitoring operation of a

software program in a network environment comprising: an execution component for

executing the software program, a monitoring component for obtaining information

about actions performed by the software program, a network emulation component,

couple to the network, for emulating the behavior of at least a host providing network

services, wherein the execution component and the network emulation component

cooperate with the network in order to elicit a behavior of the software program that is

detectable by the monitoring component (See Column 6, lines 41-67, Column 7, lines 1-

18)

Schnurer et al. does not teach the execution component being coupled to an

isolated network that does not have a direct connection to another network that is not an

isolated network. Nachenburg teaches the execution component being coupled to an

isolated network that does not have a direct connection to another network that is not an

isolated network (See Column 5, lines 62-67, Column 4, lines 1-40).

It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine Schnurer et al. 's system for trapping computer viruses with Nachenburg's

method for emulating a polymorphic virus detection module which will allow monitoring

and disruptive network behavior prior to emulating the target program. (See

Nachenburg, Column 3, lines 37-46).

As per claim 2, Schnurer et al. and Nachenburg teach a system as in claim 1, in addition Schnurer et al. teaches the emulation component further comprises a server programmed so as to return emulated results in response to a request resulting from the software program being executed on the execution component. (See Column 7, lines 19-52)

As per claim 3, Schnurer et al. and Nachenburg teach a system as in claim 1, in addition Schnurer et al. teaches the emulation component is programmed so as to limit access by the software program to only certain resources. (See Column 3, lines 16-23)

As per claim 4, Schnurer et al. and Nachenburg teach a system as in claim 1, in addition Schnurer et al. teaches where at least one of the emulation component and monitoring component are programmed so as to provide information about the performance of the software program for the purposes of testing, debugging, performance profiling or optimization. (See Column 8, lines 20-25)

As per claim 5, Schnurer et al. and Nachenburg teach a system as in claim 1, in addition Schnurer et al. teaches where at least one of the emulation component and monitoring component are programmed so as to provide information about actions of the software program for the purposes of reverse engineering or otherwise determining the function and behavior of the software program. (See Column 8, lines 1-19)

As per claim 6, Schnurer et al. and Nachenburg teach a system as in claim 1, in addition Schnurer et al. teaches where at least one of the emulation component and monitoring component are programmed so as to provide information about actions of

the software program for the purposes of detecting a presence of an undesirable

software entity within the software program. (See Column 4, lines 27-36)

As per claims 7 and 8, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches wherein the undesirable software entity comprises at

least one of a worm or a virus. (See Column 5, lines 62-67, Column 1, lines 1-7)

As per claim 9, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches where the elicited behavior of the software program

comprises self-replication. (See Column 7, lines 12-15)

As per claim 10, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches where the elicited behavior of the software program

comprises viral or malicious activity. (See Column 4, lines 37-57)

As per claim 11, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches the server is programmed to determine what result to

return based at least in part on a result of a corresponding real query sent to a

corresponding real server on a corresponding real, non-isolated network. (See Column

8, lines 21-35)

As per claim 12, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches the server is programmed to function as an optimistic

host. (See Column 8, lines 50-59)

As per claim 13, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches where the server comprises at least one of a real or an

emulated Web server. (See Column 5, lines 29-32)

Regarding claim 14, Schnurer et al. and Nachenburg teach a system as in claim 2, but

do not teach said server comprises at least one of a real or emulated http, ftp, imap4,

pop3, nntp, news, irc, chat, smtp, mail and mailbox server. Examiner takes official

notice that http, ftp, imap4, pop3, nntp, news, irc, chat, smtp, mail and mailbox servers

are well known in the art. It would have been obvious to one of ordinary skill in the art to

use one of these servers in order to obtain efficient network communication.

Regarding claim 15, Schnurer et al. and Nachenburg teach a system as in claim 2, but

do not teach a real or emulated router. Examiner takes official notice that routers used

in conjunction with servers are well know in the art. It would have been obvious to one

of ordinary skill to use a router with a server in order to expedite message delivery.

Regarding claim 16, Schnurer et al. and Nachenburg teach a system as in claim 2, but

do not teach said server comprises at least one of a real or emulated DNS, WINS, or

other Name server. Examiner takes official notice that DNS, WINS, or other Name

servers are well known in the art. It would have been obvious to one of ordinary skill in

the art to use one of these servers in order to associate a computer's host name with its

address.

Regarding claim 17, Schnurer et al. and Nachenburg teach a system as in claim 2, but

do not teach said server comprises at least one of a real or emulated SNMP server.

Examiner takes official notice that SNMP servers are well known in the art. It would

have been obvious to one of ordinary skill in the art to use SNMP in order to be able to

monitor the activity in the various devices on the network and report to the network

console workstation.

Regarding claim 18, Schnurer et al. and Nachenburg teach a system as in claim 2, but

do not teach said server comprises at least one of a real or emulated NetBIOS server.

Examiner takes official notice that NetBIOS servers are well known in the art. It would

have been obvious to one of ordinary skill in the art to use NetBIOS servers in order to

provide application programs with a uniform set of commands for requesting the lower-

level network services required to conduct sessions between nodes on a network and to

transmit information back and forth.

Regarding claim 19, Schnurer et al. and Nachenburg teach a system as in claim 2, but

do not teach said server comprises at least one of a real or emulated server that

operates in accordance with SMB, NES or other distributed file system protocols.

Examiner takes official notice that SMB, NES or other distributed file system protocols

are well known in the art. It would have been obvious to one of ordinary skill in the art to

use SMB, NES or other distributed file system protocols in order to define a series of

commands that allow information to be passed between computers.

Regarding claim 20, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches where said monitoring component comprises a monitor

programmed to record certain information or types of information that flow across the

isolated network as a result of the execution of the software program. (See Column 8,

lines 36-49)

Regarding claim 21, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches where said monitoring component comprises a monitor

programmed to record at least one of certain operating system level or application level

activities or types of activities that occur in real or emulated host computers as a result

of the execution of the software program. (See Column 8, lines 1-20)

Regarding claim 22, Schnurer et al. and Nachenburg teach a system as in claim 2, in

addition Schnurer et al. teaches where said monitoring component comprises a monitor

programmed to record at least certain activities or types of activities that occur in said

server as a result of the execution of the software program. (See Column 7, lines 52-67)

Regarding claim 23, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches where said monitoring component comprises at least

one event handler programmed so as to obtain control when certain events or types of

events occur. (See Column 6, lines 63-67, Column 7, lines 1-5)

Regarding claim 24, Schnurer et al. and Nachenburg teaches a system as in claim 23,

in addition Schnurer et al. teaches where the certain events or types of events comprise

at least one of creation of a new file in a filesystem, receipt of mail, an opening of mail, a

posting of news, an opening of a new socket connection, an execution of a particular

application, and an alteration of a system registry. (See Column 6, lines 8-49)

Regarding claim 25, Schnurer et al. and Nachenburg teach a system as in claim 1, in

addition Schnurer et al. teaches where said emulation component further comprises a

system activity emulation component for emulating typical or specific activity on at least

one of said isolated network and a real or emulated host computer. (See Column 7,

lines 19-52)

Regarding claim 26, Schnurer et al. and Nachenburg teach a system as in claim 25, in

addition Schnurer et al. teaches where the typical or specific activity comprises at least

one of sending mail, opening mail, opening or execution of a mail attachment, entry of

keystrokes, issuing of user commands, execution of a particular application, rebooting a

real or emulated host computer, restarting a real or emulated host computer,

reinitialization of a real or emulated host computer, posting of news, participation in real-

time messaging, and a transfer of files. (See Column 7, lines 25-37)

Claims 27-46 are rejected because of similar rationale outlined above.

Conclusion

6.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. Bishop et al. "An Isolated Network for Research" discloses a

model used to protect the information on an isolated network.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Courtney D. Fields whose telephone number is 571-

272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off

every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free).

cdf
March 18, 2005

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER